JOURNAL
de Théorie des Nombres
de BORDEAUX
anciennement Séminaire de Théorie des Nombres de Bordeaux

Bernat Plans, Núria Vila

Galois covers of $\mathbb{P}^1$ over $\mathbb{Q}$ with prescribed local or global behavior by specialization

Tome 17, n° 1 (2005), p. 271-282.

<http://jtnb.cedram.org/item?id=JTNB_2005__17_1_271_0>

Journal de Théorie des Nombres
de Bordeaux **17** (2005), 271–282

Galois covers of $\mathbb{P}^1$ over $\mathbb{Q}$ with prescribed local or global behavior by specialization

par Bernat PLANS et Núria VILA

Résumé. On considère des versions raffinées du Problème Inverse de Galois. Nous étudions le comportement local et global des spécialisations rationnelles de quelques revêtements galoisiens finis de $\mathbb{P}^1_{\mathbb{Q}}$.

Abstract. This paper considers some refined versions of the Inverse Galois Problem. We study the local or global behavior of rational specializations of some finite Galois covers of $\mathbb{P}^1_{\mathbb{Q}}$.

1. Introduction

The Inverse Galois Problem asks whether, for an arbitrary finite group G, there exists a Galois extension $L/\mathbb{Q}$ with Galois group isomorphic to G. Such an extension $L/\mathbb{Q}$ will be called a *G-extension of* $\mathbb{Q}$. Usually, this also means that an isomorphism $G \cong \mathrm{Gal}(L/\mathbb{Q})$ has been fixed. Stronger versions of the Inverse Galois Problem can be obtained imposing additional restrictions on the local behavior at finitely many primes. For example, we may require all primes in a finite set S to be unramified in $L/\mathbb{Q}$. For every finite solvable group G and every finite set S, it is known that this is always possible (cf. [13, Thm. 6.2]). Also, following Birch [4], one can require all ramified primes to be tamely ramified; this is known as the Tame Inverse Galois Problem.

A natural way to obtain G-extensions of $\mathbb{Q}$ is by rational specialization of Galois covers of $\mathbb{P}^1_{\mathbb{Q}}$ with Galois group G, by Hilbert's irreducibility Theorem. Roughly, the present paper considers "what kind" of G-extensions of $\mathbb{Q}$ arise by specialization of such a cover. More precisely, in Section 2, we consider various G-covers of $\mathbb{P}^1_{\mathbb{Q}}$ and we look for rational G-specializations which satisfy some extra prescribed local conditions at finitely many primes, such as non-ramification or tameness. The groups we treat comprise, among others, symmetric and alternating groups, small Mathieu groups and finite central extensions for all of them. It is known that, for some particular groups G, there always exist G-covers which admit some specialization

Research partially supported by MCYT grant BFM2003-01898.

with "arbitrary" prescribed local behavior at finitely many primes. For instance, if there exists a generic G-extension over $\mathbb{Q}$ (see [24] or [11]), as for the symmetric group $G = S_n$, then it suffices to specialize at a line through two well-chosen points: one giving the prescribed behavior (weak approximation) and the other one to ensure regularity. Of course, the only "admissible" local behaviors at a prime p are those corresponding to Galois extensions of $\mathbb{Q}_p$ with Galois group contained in G. Even then, given a finite group G, not every "admissible" local behavior must be globally realizable, as shown by Wang's counterexample to Grunwald's Theorem (see, for example, [24, Thm. 5.11]).

Most of the covers we treat are obtained by the so-called rigidity method with three rational branch points, deduced from a rigid triple of rational conjugacy classes in G (see [14]). At the outset, this means that some local behaviors cannot occur. Actually, if G is a (centerless) group with more than 6 elements, then such a cover never admits totally real specializations (cf. [25]). On the other hand, in this rigid case, it follows from a result of Beckmann [2] that there are always specializations unramified at an arbitrary prefixed finite prime p, provided p does not divide the order of G. However, Birch [4] suggests that specializations of these rigid covers are likely to be wildly ramified.

In Section 3 we report on some results concerning the existence of G-covers of $\mathbb{P}^1_{\mathbb{Q}}$ with a (global) prescribed G-specialization. In other words, we consider the arithmetic lifting property for G over $\mathbb{Q}$.

Let us briefly introduce the basic terminology.

Let G be a finite group and let $X_{\mathbb{Q}}$ be a geometrically irreducible, nonsingular, projective curve over $\mathbb{Q}$. A finite dominant morphism $X_{\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}}$ over $\mathbb{Q}$ will be called a *G-cover of $\mathbb{P}^1_{\mathbb{Q}}$ over $\mathbb{Q}$*, or simply a *G-cover*, whenever the corresponding function field extension $\mathbb{Q}(X_{\mathbb{Q}})/\mathbb{Q}(T)$ is a Galois extension and an isomorphism $G \cong \mathrm{Gal}(\mathbb{Q}(X_{\mathbb{Q}})/\mathbb{Q}(T))$ has been fixed.

The *specialization* of a G-cover $X_{\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}}$ at an unramified rational point $t \in \mathbb{P}^1(\mathbb{Q})$ will be the field extension $X_t/\mathbb{Q}$, where X_t can be defined as the compositum of all residue fields of $X_{\mathbb{Q}}$ at the points over t. This is a Galois extension of $\mathbb{Q}$ with Galois group isomorphic to some subgroup of G.

Note that, in order to study the ramification at finite primes in number fields, we will freely make use of Ore's basic results on Newton polygons and associated polynomials, which can be found in [20] or [17]. In addition, we use standard Atlas [1] notations for conjugacy classes of finite groups.

2. Specializations with prescribed local behavior

Let G be a finite group and let $X_{\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}}$ be a G-cover. Let p be a rational prime. The specializations of $X_{\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}}$ at two unramified points $t_1, t_2 \in \mathbb{P}^1(\mathbb{Q})$ are locally (at p) isomorphic, provided t_1 and t_2 are p-adically

close enough. This follows from Krasner's Lemma (cf. [24, Lemma 5.5]). Then, since Hilbert's Irreducibility Theorem is known to be compatible with the weak approximation Theorem (and also with the strong approximation Theorem, see [19] or [10]), the next proposition follows.

Proposition 2.1. *Let G be a finite group and let $X_{\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}}$ be a G-cover over $\mathbb{Q}$. Let S be a finite set of rational primes (possibly including $p = \infty$). Assume that, for each $p \in S$, a finite extension $L_p/\mathbb{Q}_p$ has been fixed ($\mathbb{Q}_\infty = \mathbb{R}$). Then, the following properties are equivalent:*

(i) *For each $p \in S$, there exists $t_p \in \mathbb{P}^1(\mathbb{Q})$ such that L_p is isomorphic to the completion at p of X_{t_p}.*

(ii) *There exists $t \in \mathbb{P}^1(\mathbb{Q})$ such that $\mathrm{Gal}(X_t/\mathbb{Q}) \cong G$ and, for every $p \in S$, L_p is isomorphic to the completion at p of X_t.*

Hence, in order to prove (or disprove) the existence of specializations with Galois group G and with prescribed local behavior at finitely many primes, we may look at one prime at a time and we do not have to worry about the corresponding Galois group.

Let us begin with the symmetric and alternating groups. It is well known that, if $(n,k) = 1$, then $(nA, 2A, C^{(k)})$ is a rigid triple of (rational) conjugacy classes of the symmetric group S_n (cf. [28]).

Proposition 2.2. *Let $k < n$ be coprime positive integers and let $X_{\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}}$ be an S_n-cover obtained from the rigid triple $(nA, 2A, C^{(k)})$. Let S be a finite set of prime numbers. Then, there exist rational points $t \in \mathbb{P}^1(\mathbb{Q})$ such that the specialized field extension $X_t/\mathbb{Q}$ is unramified at S and $\mathrm{Gal}(X_t/\mathbb{Q}) \cong S_n$.*

Proof. We can assume that the branch points are $\infty, \frac{k^k(k-n)^{n-k}}{n^n}, 0$. Once these have been fixed, the S_n-cover of $\mathbb{P}^1_{\mathbb{Q}}$ is unique (by rigidity). Hence, it suffices to consider the Galois closure of the following cover (see [26, 8.3.1])

$$\mathbb{P}^1_{\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}} \quad , \qquad X \mapsto X^k(X-1)^{n-k},$$

which has the appropriate ramification description. It is easy to check that there exist $a, b \in \mathbb{Z}$ such that no prime in S divides the discriminant of $X^k(X-a)^{n-k} + b$. The result then follows from Proposition 2.1. □

Let $H \subset G$ be a subgroup of index 2. For every G-cover $X_{\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}}$ with only three branch points, all of them being $\mathbb{Q}$-rational, the fixed field $\mathbb{Q}(X_{\mathbb{Q}})^H$ must be purely transcendental over $\mathbb{Q}$. This follows from Riemann-Hurwitz's formula (see, for example, [26, Lemma 4.5.1]). One thus obtains

an H-cover $Y_{\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}}$. However, the existence of specializations with some prescribed local behavior is not necessarily preserved in this process. For example, we have:

Proposition 2.3. *Let $k < n$ be coprime positive integers and assume that $n \equiv 4 \pmod 8$. Let $X_{\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}}$ be an S_n-cover obtained from the rigid triple $(nA, 2A, C^{(k)})$ and let $Y_{\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}}$ be the corresponding A_n-cover. Then, the specializations $Y_t/\mathbb{Q}$ are wildly ramified at $p = 2$, for every (unramified) $t \in \mathbb{P}^1(\mathbb{Q})$.*

Proof. It suffices to prove that, for every polynomial of type

$$f(X) := X^k(X-a)^{n-k} + b \in \mathbb{Z}[X]$$

with non-zero square discriminant in $\mathbb{Q}$, its splitting field $\mathbb{Q}_f/\mathbb{Q}$ is wildly ramified at $p = 2$.

Up to rational squares, the discriminant $D(f)$ of $f(X)$ is $a^n k^k (k-n)^{n-k} + bn^n$. Since $k^k(k-n)^{n-k} \equiv 5 \pmod 8$ and $D(f)$ is a non-zero square integer, it must be $v_2(bn^n) \leq v_2(a^n)$. This allows us to assume that $v_2(b) < n$. Note that $v_2(a) \geq 2$.

Let us first consider the case b even. The Newton polygon (at $p = 2$) of $f(X)$ has only one side in this case, with slope $-\frac{v_2(b)}{n}$. Hence, if $v_2(v_2(b)) < 2$, then $p = 2$ is wildly ramified in $\mathbb{Q}_f/\mathbb{Q}$. From now on we assume $v_2(v_2(b)) \geq 2$. Let $\theta \in \overline{\mathbb{Q}_2}$ be a $\frac{n}{4}$-th root of 2 and let us define

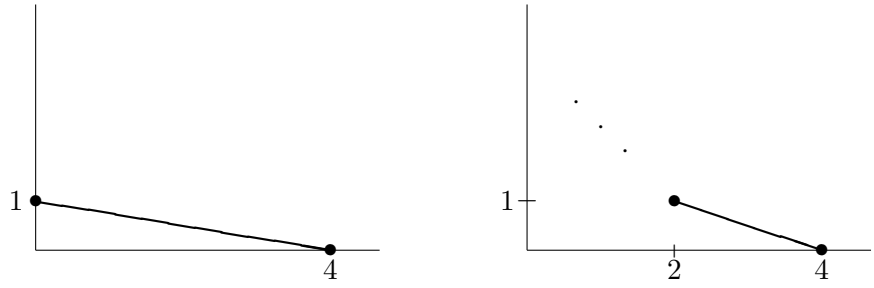
$$g(X) := \frac{1}{2^{v_2(b)}} f(\theta^{\frac{v_2(b)}{4}} X) = X^k \left(X - \frac{a}{\theta^{\frac{v_2(b)}{4}}} \right)^{n-k} + \frac{b}{2^{v_2(b)}}.$$

Under our present assumptions, it must be $v_2(bn^n) + 4 \leq v_2(a^n)$. It follows that

$$v_2\left(\frac{a}{\theta^{\frac{v_2(b)}{4}}} \right) > 2 \text{ and } \frac{b}{2^{v_2(b)}} \equiv 1 \pmod 8.$$

Hence, we obtain that $g(X+1) \equiv (X+1)^n + 1 \pmod 4$ and the Newton polygon of $g(X+1)$ has only one side, with slope $-\frac{1}{4}$. Thus, the extension $(\mathbb{Q}_2(\theta))_g/\mathbb{Q}_2$ is wildly ramified. Since $(\mathbb{Q}_2(\theta))_g = \mathbb{Q}_2(\theta) \cdot (\mathbb{Q}_2)_f$ and the extension $\mathbb{Q}_2(\theta)/\mathbb{Q}_2$ is tamely ramified, we conclude that $p = 2$ is wildly ramified in $\mathbb{Q}_f/\mathbb{Q}$.

Finally, we consider the remaining case b odd. In this case, the congruence $f(X+1) \equiv (X+1)^n + b \pmod 4$ forces the Newton polygon of $f(X+1)$ to be of one of the following types



Both cases ensure that $\mathbb{Q}_f/\mathbb{Q}$ is wildly ramified at $p = 2$. □

Remark. An analogous result holds for A_n-extensions of $\mathbb{Q}$ obtained as splitting fields of degree n trinomials (cf. [23]).

From other suitable A_n-covers of $\mathbb{P}^1_{\mathbb{Q}}$ one obtains that, for every n, there always exist A_n-extensions of $\mathbb{Q}$ unramified at all primes in an arbitrary prefixed finite set; more restrictive local behaviors can also be forced to occur (see [12] and [22]). In this direction, the best possible situation would be that every (admissible) prescribed local behavior at finitely many primes actually occurs in some A_n-extension of $\mathbb{Q}$. This Grunwald-Wang type result for A_n over $\mathbb{Q}$ is known to hold only for $n \leq 5$, as a consequence of an affirmative answer to Noether's problem for these groups (see [24] and [11]). For arbitrary n, even though no such an affirmative answer is known, nor even the existence of a generic A_n-extension over $\mathbb{Q}$, one can still obtain partial results such as the following one.

Proposition 2.4. *Let n be a positive integer and let S be a finite set of rational primes. Assume that, for each $p \in S$, a local Galois extension $L_p/\mathbb{Q}_p$ has been fixed. If all the Galois groups $\{\mathrm{Gal}(L_p/\mathbb{Q}_p)\}_{p\in S}$ are embeddable in S_{n-2}, then there exists an A_n-extension of $\mathbb{Q}$ whose completion at every $p \in S$ is isomorphic to $L_p/\mathbb{Q}_p$.*

Proof. Let A_n act on the affine n-space $\mathbb{A}^n_{\mathbb{Q}}$ by permutation of coordinates and let $\pi : \mathbb{A}^n_{\mathbb{Q}} \to \mathbb{A}^n_{\mathbb{Q}}/A_n$ be the corresponding projection. Mestre [15] showed that there exists a nonempty Zariski open subset $U \subset \mathbb{A}^n_{\mathbb{Q}}$ with the following property:

> For every $\alpha = (\alpha_1, \ldots, \alpha_n) \in U(\overline{\mathbb{Q}})$ such that $\pi(\alpha)$ is a $\mathbb{Q}$-rational point, there exists an A_n-cover $C_{\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}}$ whose specialization at some $t \in \mathbb{P}^1(\mathbb{Q})$ is $C_t = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$.

Since S_{n-2} can be embedded into A_n, every S_{n-2}-extension of $\mathbb{Q}$ can be obtained as $\mathbb{Q}(\alpha)$, for some $\alpha \in \mathbb{A}^n(\overline{\mathbb{Q}})$ such that $\pi(\alpha)$ is a $\mathbb{Q}$-rational point.

We can assume, moreover, that $\alpha \in U(\overline{\mathbb{Q}})$ (see, for example, [27, Lemma 4.5]). The result then follows from Proposition 2.1, taking into account that a Grunwald-Wang type result for the symmetric group S_{n-2} over $\mathbb{Q}$ always holds (cf. [24]). □

Remark. The above result obviously also holds if one replaces S_{n-2} by a subgroup $G \subset A_n$, provided a Grunwald-Wang type result holds for G.

Let us remark that the given proof is based on the fact that, as a consequence of Mestre's result, the general form of the arithmetic lifting property for A_n over $\mathbb{Q}$ holds (see Section 3).

We next consider the Mathieu group M_{22} and its automorphism group $\mathrm{Aut}(M_{22})$. The situation is formally similar to the first examples of this section, in the sense that $\mathrm{Aut}(M_{22})$ admits a rigid triple of rational conjugacy classes and M_{22} is a subgroup of index 2 (and $S_n = \mathrm{Aut}(A_n)$, if $n \neq 2, 6$). More precisely, $(2B, 4C, 11A)$ is such a triple in $\mathrm{Aut}(M_{22})$ (cf. [14]).

Proposition 2.5. *Let $X_{\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}}$ be an $\mathrm{Aut}(M_{22})$-cover obtained from the rigid triple $(2B, 4C, 11A)$ and let $Y_{\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}}$ be the corresponding M_{22}-cover. Then:*

(a) *There exist tamely ramified $\mathrm{Aut}(M_{22})$-specializations $X_t/\mathbb{Q}$. Moreover, one can also require $X_t/\mathbb{Q}$ being unramified at all prime numbers in an arbitrary prescribed finite set not containing $p = 11$.*

(b) *The specializations $Y_t/\mathbb{Q}$ are wildly ramified at $p = 2$, for every (unramified) $t \in \mathbb{P}^1(\mathbb{Q})$.*

Proof. As above, it suffices to consider a concrete $\mathrm{Aut}(M_{22})$-cover with the right ramification type. Following [14] we take the Galois closure of the cover

$$\mathbb{P}^1_{\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}}, \quad X \mapsto \frac{p(X)^4 q(X)^2}{r(X)^{11}},$$

where $p(X) = 5X^4 + 34X^3 - 119X^2 + 212X - 164$, $q(X) = 19X^3 - 12X^2 + 28X + 32$ and $r(X) = X^2 - X + 3$.

In terms of function fields, we consider the splitting field over $\mathbb{Q}(T)$ of the polynomial $F(T, X) := p(X)^4 q(X)^2 - T \cdot r(X)^{11}$ or, equivalently, the splitting field of the monic polynomial

$$f(T, X) := a^{21} F\left(T, \frac{X}{a}\right) \in \mathbb{Z}[X, T],$$

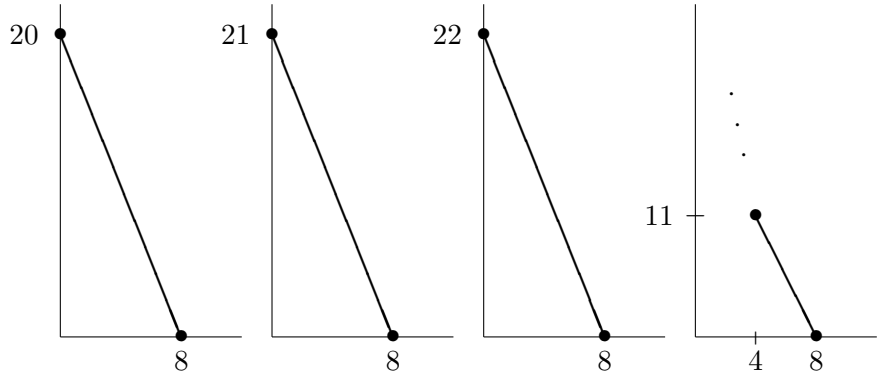
where $a \in \mathbb{Z}[T]$ is the leading coefficient of $F(T, X)$.

In statement (a), we only have to study the local behavior at $p = 2$ and $p = 11$, since these are the only common prime factors of $D(f(2, X))$ and $D(f(3, X))$.

The specialization at $t = 1$ is not ramified at $p = 2$, since the reduction modulo 2 of $X^{22} f(1, \frac{1}{X})$ is a (degree 22) separable polynomial in $\mathbb{F}_2[X]$.

For $p = 11$, we have that $f(11^4, X) \equiv (X + 9)^{22} \pmod{11}$ and the $(X + 9)$-Newton polygon of $f(11^4, X)$ has two sides with slopes $-\frac{3}{4}$ and $-\frac{2}{3}$. In particular, this means that, for every root $\theta \in \overline{\mathbb{Q}}$ of $f(11^4, X)$, the ramification index in $\mathbb{Q}(\theta)/\mathbb{Q}$ at every prime over $p = 11$ must be divisible by either 3 or 4. Hence, $p = 11$ is tamely ramified in $\mathbb{Q}(\theta)/\mathbb{Q}$, so also in the splitting field over $\mathbb{Q}$ of $f(11^4, X)$.

In order to obtain statement (b), we will prove that $p = 2$ is wildly ramified in the splitting field over $\mathbb{Q}$ of $f(t, X)$, for every $t \in \mathbb{Q}$ such that the discriminant $D(f(t, X))$ is a non-zero rational square. It can be checked that, up to squares in $\mathbb{Q}(T)$, the discriminant of $f(T, X)$ is $11T(2^{22} - T)$. Hence, $D(f(t, X))$ is a rational square if and only if $t = \frac{2^{22}}{11s^2+1}$, for some $s \in \mathbb{Q}$. This forces $v_2(t) \geq 20$. As a consequence, $f(t, X) \equiv X^{14}(X - 1)^8 \pmod{2}$ and the $(X-1)$-Newton polygon ($p = 2$) of $f(t, X)$ must be of one of the following types



In each of these cases there is a side whose slope has negative 2-adic valuation. Hence, $p = 2$ must be wildly ramified in the splitting field of $f(t, X)$ over $\mathbb{Q}$. □

We will now consider the smallest Mathieu groups M_{11} and M_{12}. The covers considered below can be found in [14]. The triple $(4A, 4A, 10A)$ in M_{12} is known to be rational. Even though it is not rigid in a strict sense, it also appears as the ramification type of an M_{12}-cover $X_{\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}}$ ramified only at three (non-rational) points. More concretely, one can obtain such a cover as the Galois closure of the morphism $\pi : \mathbb{P}^1_{\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}}$ given by

$X \mapsto \frac{h(X)}{X^2}$, with

$$\begin{aligned} h(X) = {} & X^{12} + 20.5X^{11} + 162.5^2X^{10} + 3348.5^2X^9 + 35559.5^2X^8 \\ & +5832.5^4X^7 - 84564.5^3X^6 - 857304.5^3X^5 + 807003.5^3X^4 \\ & +1810836.5^4X^3 - 511758.5^4X^2 + 2125764.5^4X + 531441.5^4. \end{aligned}$$

In a natural way, this also defines an M_{11}-cover $Y_{\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}}$.

Proposition 2.6. *Let $X_{\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}}$ be the above M_{12}-cover and let $Y_{\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}}$ be the corresponding M_{11}-cover. Then:*

(a) *There exist tamely ramified M_{12}-specializations $X_t/\mathbb{Q}$. Moreover, one can also require $X_t/\mathbb{Q}$ to be unramified at all prime numbers in an arbitrary prescribed finite set not containing $p = 5$.*

(b) *There exist tamely ramified M_{11}-specializations $Y_t/\mathbb{Q}$. Moreover, one can also require $Y_t/\mathbb{Q}$ to be unramified at all prime numbers in an arbitrary prescribed finite set not containing $p = 5$.*

Proof. Rational specializations of the M_{11}-cover $Y_{\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}}$ are nothing but specializations of $X_{\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}}$ at points in $\pi(\mathbb{P}^1(\mathbb{Q}))$. Hence, by Proposition 2.1, statement (a) follows from statement (b).

It suffices to prove that, for every prime number $p \neq 5$ (resp. $p = 5$), there exists $t \in \mathbb{Q}$ such that the polynomial

$$f(t, X) := h(X) - \frac{h(t)}{t^2}X^2$$

has non-zero discriminant and splitting field over $\mathbb{Q}$ unramified at p (resp. tamely ramified at $p = 5$).

The only common prime factors of $D(f(1, X))$ and $D(f(-1, X))$ are $p = 2, 3, 5$.

Modulo $p = 3$, the factorization of $f(1, X)$ is

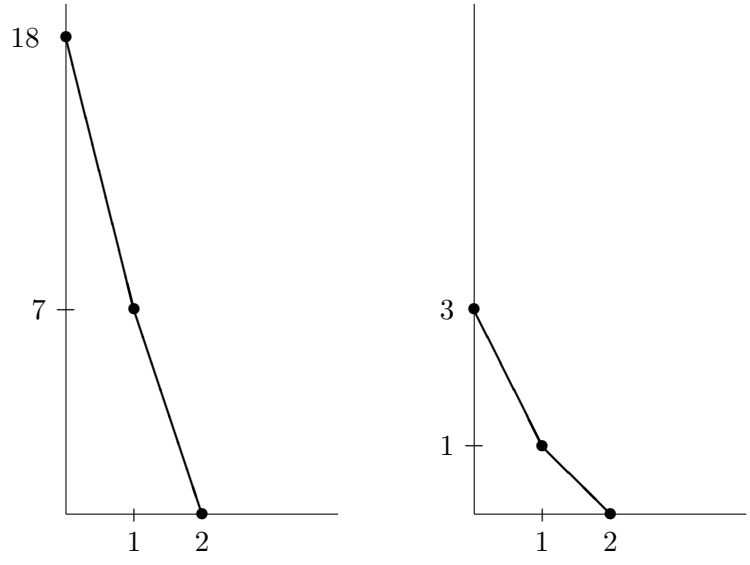
$$X^2(2 + X)(2 + X + X^2 + X^3)(1 + 2X + X^2 + 2X^3 + X^5 + X^6).$$

The Newton polygon ($p = 3$) of $f(1, X)$ with respect to $(X + 3^6)$ has only one side $\mathcal{S}$, whose first and last points are $(0, 12)$, $(2, 0)$; hence $\mathcal{S}$ has integer slope. The polynomial associated to $\mathcal{S}$ is $2 + Y + Y^2 \in \mathbb{F}_3[Y]$, so it has no multiple roots. We conclude that $p = 3$ does not ramify in the splitting field of $f(1, X)$ over $\mathbb{Q}$.

Now take $p = 5$. We have $f(1, X) \equiv X^2(1 + X)^5(4 + X)^5 \pmod 5$. As we already know that $X = 1$ is a root of $f(1, X)$, wild ramification at $p = 5$ in the splitting field of $f(1, X)$ over $\mathbb{Q}$ can only "come" from the factor $(1 + X)^5$. It follows that there is no wild ramification at all, since the Newton polygon ($p = 5$) of $f(1, X)$ with respect to $(1 + X)$ has two sides (whose slopes are -1 and $-1/4$).

Finally, we must consider $p = 2$. In order to prove that 2 does not ramify when we specialize at $t = \frac{1}{2}$, we define $f(X) := 2^{12}.f\left(\frac{1}{2}, \frac{X}{2}\right) \in \mathbb{Z}[X]$ and

we note that it has $X = 1$ as a root. The factorization of $f(X)$ modulo 2 is $X^2(1+X)^2(1+X+X^2+X^3+X^4)^2$. To finish the proof, we check that the Newton polygons ($p = 2$) with respect to $(X+2^6)$ and $(1+X+X^2+X^3+X^4)$ are, respectively,



□

From the above results, various finite groups G can be realized as Galois groups of tamely ramified extensions of $\mathbb{Q}$. Moreover, if such a tame G-extension of $\mathbb{Q}$ gives rise to a solvable finite central embedding problem, then we can deduce tame realizations over $\mathbb{Q}$ for the extension group too. To do so, we use class field theory in order to obtain these realizations by suitable twist of an arbitrary solution (cf. [21]). In some cases, we can even ensure that a realization of this type arises by specialization of a Galois cover of $\mathbb{P}^1_{\mathbb{Q}}$ with the same Galois group. Among the groups treated above, the easiest case corresponds to the Mathieu group M_{11}. It is a perfect (simple) group with trivial Schur multipliers; therefore its realizations always give rise to solvable finite central embedding problems.

Proposition 2.7. *(cf.* [21]*) Let G be a finite central extension group of one of the following groups:*

- *the symmetric group S_n, $n \geq 5$.*
- *the alternating group A_n, $n \geq 5$.*
- *the Mathieu groups M_{11} and M_{12}.*

Then, there exists a G-cover $X_{\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}}$ whose specialization at some $t \in \mathbb{P}^1(\mathbb{Q})$ is a tamely ramified G-extension of $\mathbb{Q}$.

Remark. For central extension groups of S_n, one can also require that all prime numbers in an arbitrary prefixed finite set S do not ramify. From Proposition 2.6, we can prove the analogous result for M_{11} and M_{12}, with the obvious additional hypothesis $5 \notin S$. For central extensions of the alternating group A_n, $n \neq 6, 7$, we have even stronger results, similar to Proposition 2.4 (following from Proposition 3.2 below).

3. Globally prescribed specializations

Black [6] conjectures that, for every finite group G and every field K, all G-extensions of K arise by specialization of G-covers of $\mathbb{P}^1_K$. This is also currently known as the Beckmann-Black problem. Whenever this holds for a pair (G, K), we say that G has the *arithmetic lifting property* over K.

Dèbes [9] proved that, from an affirmative answer to the Beckmann-Black problem for a finite group G over every field, it follows that there exists some G-cover of $\mathbb{P}^1_K$ for every field K.

The arithmetic lifting property has been proved for the following pairs (G, K), among others.

- G finite abelian and K a number field (cf. [3]) and, more generally, K an arbitrary field (cf. [8]).
- $G = S_n$ the symmetric group and $K = \mathbb{Q}$ (cf. [3]) and, more generally, if there exists a generic extension for G over K (cf. [5]).
- G an arbitrary finite group and K a PAC field (cf. [9]) and, more generally, K a large field (cf. [7], [18]).
- $G = \mathrm{PSL}_2(\mathbb{F}_7)$ and K an arbitrary field of characteristic 0 (cf. [16]).

Black [6] also remarked that the alternating group A_n has the arithmetic lifting property over every field K of characteristic 0. This follows from a general construction of A_n-covers of $\mathbb{P}^1_K$ given by Mestre [15], as in the proof of Proposition 2.4. Moreover, Mestre's A_n-extensions of $K(T)$ have the following remarkable property: given a finite central extension group G of A_n, the corresponding embedding problem (over $K(T)$) has constant obstruction, provided 3 does not divide the order of the kernel. For almost every n, A_n is a perfect group and 3 does not divide the order of its Schur multipliers. Hence, Mestre's construction gives a natural starting point when trying to "lift" the arithmetic lifting property from A_n to its finite central extensions. Taking advantage of the fact that, generically, the order of the Schur multipliers of A_n is precisely 2, we proved:

Proposition 3.1. *(cf.* [21]*) Let G be a finite central extension group of A_n, with $n \neq 4, 6, 7$. Then, the arithmetic lifting property holds for G over every field of characteristic* 0.

Most of the above pairs (G, K) even satisfy the following *general form of the arithmetic lifting property*: given a subgroup $H \subseteq G$, every H-extension of K arises by specialization of a G-cover of $\mathbb{P}^1_K$.

Remark. This general form can be rephrased to say that every G-extension of *algebras* L/K arises by specialization of a G-cover of $\mathbb{P}^1_K$. To do so, one has to define the specialization of a G-cover $X_K \to \mathbb{P}^1_K$ at an unramified point $t \in \mathbb{P}^1(K)$ merely as the (algebra) extension of K corresponding to the fiber over t. It is always a Galois extension with group G.

For finite central extension groups of A_n we have:

Proposition 3.2. *(cf.* [21]*) Let G be a finite central extension group of A_n, with $n \neq 4, 6, 7$. Then, the general form of the arithmetic lifting property holds for G over every hilbertian field of characteristic* 0*.*

Remark. Note that the general form of the arithmetic lifting property for G over $\mathbb{Q}$ directly leads to partial Grunwald-Wang type results for G over $\mathbb{Q}$ (as in Proposition 2.4).

References

[1] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, R. A. Wilson, *Atlas of Finite Groups*. New York: Clarendon press, 1985.

[2] S. Beckmann, *On extensions of number fields obtained by specializing branched coverings*. J. Reine Angew. Math. **419** (1991), 27–53.

[3] S. Beckmann, *Is every extension of $\mathbb{Q}$ the specialization of a branched covering?* J. Algebra **165** (1994), 430–451.

[4] B. Birch, *Noncongruence subgroups, Covers and Drawings*. Leila Schneps, editor, The Grothendieck theory of dessins d'enfants. Cambridge Univ. Press (1994), 25–46.

[5] E. Black, *Deformations of dihedral 2-group extensions of fields*. Trans. Amer. Math. Soc. **351** (1999), 3229–3241.

[6] E. Black, *On semidirect products and the arithmetic lifting property*. J. London Math. Soc. (2) **60** (1999), 677–688.

[7] J.-L. Colliot-Thélène, *Rational connectedness and Galois covers of the projective line*. Ann. of Math. **151** (2000), 359–373.

[8] P. Dèbes, *Some arithmetic properties of algebraic covers*. H. Völklein, D. Harbater, P. Müller, and J. G. Thompson, editors, Aspects of Galois theory. London Math. Soc. LNS **256** (2). Cambridge Univ. Press (1999), 66–84.

[9] P. Dèbes, *Galois Covers with Prescribed Fibers: the Beckmann-Black Problem*. Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) **28** (1999), 273–286.

[10] P. Dèbes, *Density results for Hilbert subsets*. Indian J. pure appl. Math. **30** (1) (1999), 109–127.

[11] C. U. Jensen, A. Ledet, N. Yui, *Generic polynomials*. Cambridge Univ. Press, Cambridge, 2002.

[12] J. Klüners, G. Malle, *A database for field extensions of the rationals*. LMS J. Comput. Math. **4** (2001), 182–196.

[13] J. Klüners, G. Malle, *Counting nilpotent Galois extensions*. J. reine angew. Math. **572** (2004), 1–26.

[14] G. Malle, B. H. Matzat, *Inverse Galois Theory*. Springer, Berlin, 1999.

[15] J.-F. Mestre, *Extensions régulières de $\mathbb{Q}(T)$ de groupe de Galois $\widetilde{A}_n$*. J. Algebra **131** (1990), 483–495.

[16] J.-F. Mestre, *Relèvement d'extensions de groupe de Galois* $\mathrm{PSL}_2(\mathbb{F}_7)$. Preprint (2004), arXiv:math.GR/0402187.
[17] J. Montes, E. Nart, *On a Theorem of Ore*. J. Algebra **146** (1992), 318–334.
[18] L. Moret-Bailly, *Construction de revêtements de courbes pointées*. J. Algebra **240** (2001), 505–534.
[19] Y. Morita, *A Note on the Hilbert Irreducibility Theorem*. Japan Acad. Ser. A Math. Sci. **66** (1990), 101–104.
[20] Ö. Ore, *Newtonsche Polygone in der Theorie der algebraischen Körper*. Math. Ann. **99** (1928), 84–117.
[21] B. Plans, *Central embedding problems, the arithmetic lifting property and tame extensions of* $\mathbb{Q}$. Internat. Math. Res. Notices **2003** (23) (2003), 1249–1267.
[22] B. Plans, N. Vila, *Tame* A_n*-extensions of* $\mathbb{Q}$. J. Algebra **266** (2003), 27–33.
[23] B. Plans, N. Vila, *Trinomial extensions of* $\mathbb{Q}$ *with ramification conditions*. J. Number Theory **105** (2004), 387–400.
[24] D. Saltman, *Generic Galois extensions and problems in field theory*. Adv. Math. **43** (1982), 250–283.
[25] J.-P. Serre, *Groupes de Galois sur* $\mathbb{Q}$. Sém. Bourbaki 1987-1988, no 689.
[26] J.-P. Serre, *Topics in Galois theory*. Jones and Bartlett, Boston, 1992.
[27] R. Swan, *Noether's problem in Galois theory*. J. D. Sally and B. Srinivasan, editors, Emmy Noether in Bryn Mawr. Springer (1983), 21–40.
[28] N. Vila, *On central extensions of* A_n *as Galois group over* $\mathbb{Q}$. Arch. Math. **44** (1985), 424–437.

Bernat Plans
Dept. de Matemàtica Aplicada I
Universitat Politècnica de Catalunya
Av. Diagonal, 647
08028 Barcelona, Spain
E-mail : bernat.plans@upc.edu

Núria Vila
Dept. d'Àlgebra i Geometria
Universitat de Barcelona
Gran Via de les Corts Catalanes, 585
08007 Barcelona, Spain
E-mail : nuriavila@ub.edu